

8-17-00

A

-1-

Attorney Docket No. 5437-015CIP
Client Ref: P2703 CIP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BOX NEW APP
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

jc893 U.S. PTO
09/639385
08/14/00

Sir: This is a request for filing a

- ☒ Continuation-in-part (CIP) application under 37 C.F.R. '1.53(b), of copending prior application Serial No. 08/946,036, filed on October 7, 1997 of Jonathan P. Krueger, Inventor for APPARATUS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR FILTERING INFORMATION
(title of invention)

1. ☐ A verified statement to establish Small Entity status under 37 CFR 1.9 and 1.27
- ☐ is enclosed
- ☐ was filed in prior application Serial No. _____ and such status is still proper and desired (37 CFR 1.28(a)).

2. ☒ The filing fee is calculated below:

CLAIMS AS FILED, LESS ANY CLAIMS CANCELLED BY PRELIMINARY AMENDMENT AND/OR AMENDMENT BELOW

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	18 - 20 =	0	X \$ 18 =	\$ 0
	INDEPENDENT	4 - 3 =	1	X \$ 78 =	\$ 78.00
	MULTIPLE DEPENDENT CLAIMS			+ \$260 =	\$ 0
	BASIC FEE				\$ 690.00
	TOTAL OF ABOVE CALCULATIONS=				\$ 768.00
	<input checked="" type="checkbox"/> Recordation of Assignment				\$ 40.00
	TOTAL				\$ 808.00

3. ☒ A check in the amount of \$ 808.00 is enclosed.

jc907 U.S. PTO
08/14/00

08/14/00 09/639385

4. ☒ The Commissioner is hereby authorized to charge any fees which may be required for the papers being filed herewith, or credit any overpayment to Account No. 50-1467. A duplicate copy of this sheet is enclosed.
5. Cancel Claims _____.
6. ☒ Drawing(s) are enclosed. (10 pgs)
7. ☐ Priority of the following foreign application(s) is claimed under 35 U.S.C. 119:
- | <u>Country</u> | <u>Application No.</u> | <u>Month/Day/Year</u> |
|----------------|------------------------|-----------------------|
|----------------|------------------------|-----------------------|

The certified copy(s) of the corresponding Convention Application(s):

- ☐ were filed in prior application Serial No. _____, filed _____.
- ☐ are being submitted herewith.
- ☐ will be submitted prior to payment of the Final Fee.
8. ☒ The prior application is assigned to: Sun Microsystems, Inc..
Recordation date 10/7/1997, Reel/Frame 8841/0643.
9. ☐ A Power of Attorney by Assignee is enclosed.
10. ☒ A Declaration and Power of Attorney is enclosed. (Executed) (3 pgs)
11. ☒ The Assignment and Recordation Cover Sheet is enclosed. (4 pgs)
12. ☒ Address all future communication to:
- Law Office of John Schipper
111 North Market Street, Suite 808
San Jose, California 95113
Tel: (408) 293-9934
Fax: (408) 293-2183
10. ☐ Preliminary Amendment is enclosed.
11. ☐ Also enclosed: _____

Attorney Docket No. 5437-015CIP
Client Ref: P2703 CIP

Respectfully submitted,

LAW OFFICE OF JOHN SCHIPPER

Dated: August 14, 2000

John F. Schipper
John F. Schipper
Attorney of Record
Registration No. 26,994

111 North Market Street
Suite 808
San Jose, California 95113
Tel: (408) 293-9934
Fax: (408) 293-2183

"Express Mail" mailing number EL704750834US
Date of Deposit August 14, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Carla M. Spacher
Name

Carla M. Spacher
Signature

August 14, 2000
Date

**APPARATUS, METHODS, AND COMPUTER
PROGRAM PRODUCTS FOR
FILTERING INFORMATION**

COPYRIGHTS IN PATENT MATERIALS

Portions of this patent document contain material subject to copyright restriction. The copyright owner has no objection to facsimile reproduction of the patent document after grant, as it appears in the U.S. Patent and Trademark Offices files or records, but otherwise reserves all rights relating thereto.

TECHNICAL FIELD

The field of this application relates to apparatus, methods, and computer program products for prioritizing content and information according to transmitter origin and particularly to apparatus, methods, and computer program products for filtering content and information, such as electronic mail.

BACKGROUND OF THE INVENTION

Unsolicited and undesired electronic mail (i.e., e-mail), particularly commercial e-mail originating remotely from an organization or network removed from the receiver has been referred to as "spam." Spam is a problem because it clogs e-mail channels and communication systems with undesired content. E-mail has become a primary business communication too, but has also become a transmission method for viruses. However, increasing amounts of spam are foisted upon business communicators, preventing and interfering with legitimate content distribution. Distinguishing undesired e-mail from desired e-mail is difficult because articulation of an objective standard for the subjective notion of what is desirable and what is not desirable is complex and not easy to automate in software or electronics. A technical solution to choosing or discriminating between various items of content is thus a daunting challenge.

It is accordingly desirable to enable user and entity discrimination between local and remotely originating e-mail. It is further desirable to discriminate between e-mail originating within a selected organization or entity and e-mail originating externally to that organization or entity. It is desirable to

be able to authenticate e-mail and to discriminate between internally and externally generated e-mails. It is known currently to cancel forged messages to moderated USENET groups as per PGP Moose, as discussed in detail below in connection with Figures 3-5.

5

SUMMARY OF THE INVENTION

According to the present invention, a digital signature specific to an individual or entity is associated with selected content or information for transmission with the content to one or more recipients. According to the present invention, an entity or individual signs its own content or e-mail and checks for the presence of signatures to prioritize incoming messages, content, or e-mail. Content lacking a valid signature is identified as not having been transmitted from within the selected organization or entity. According to the present invention, a transmitting mailer signs outgoing content with a selected private key or other identification (ID) prior to transmission of the particular content. The receiver of information or content checks for a valid signature or other transmitter identifying signal upon receiving particular content. E-mail or other content that does not originate locally (within a designated entity) is still able to be received and read, but it is handled differently than locally transmitted content. For example, locally originating content is according to one embodiment of the present invention placed in a different incoming e-mail folder or is positioned at the end of a predetermined message list. This preferential treatment or prioritization of content, according to the present invention, prevents non-authorized content of which spam is a well-recognized type from clogging local entity e-mail intended primarily for communication of particular content from local entity people to other local entity people.

The signing mechanism according to one embodiment of the present invention uses a selected digital signature method such as cryptographically strong hashes, for example MD5. Thus, a sender within a particular entity or organization will sign a message or other content with a private key associated with the entity. The signature and the content are then transmitted in a common package according to one embodiment of the present invention. Thus, a message is transmitted with the private key of a selected organization. According to one

embodiment of the present invention, the signature is certified by an internal certification authority by providing the entity public and private keys to entity members in encrypted form. Mail readers and content recipients are thereby able to distinguish internal e-mail from external mail (i.e., "intramural" from "extramural" e-mail) by detecting the presence or absence of an appropriate signature in transmitted content which has been received. This approach does not rely upon an e-mail header or an IP address for such distinction, because e-mail headers and IP addresses can be "forged."

According to the present invention, different kinds of content (i.e., legitimately signed and unsigned content) are handled differently upon reception. Non-authorized material of which spam is a well recognized example is filtered intelligently into remote storage according to one embodiment of the present invention and accordingly doesn't clog communication channels within an organization which otherwise might pass through all e-mail indiscriminately without filtering out extramural e-mail. According to one embodiment of the present invention, unsigned e-mail and other received content is directed into a different folder or at the end of a message list or otherwise, separating it from know valid intramural e-mail.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1A is a flow chart of an e-mail filtering method according to the present invention.

Figure 1B is a block diagram of a computer network including a computer processing system for content filtering according to the present invention.

Figure 1C is a block diagram of a content item to be transmitted including a digital signature according to the present invention.

Figure 1D is a block diagram of a computer system which can be used as a processing system for filtering content in accordance with the present invention.

Figure 1E is a block diagram of a content association filter and certification apparatus (CAFCA) according to one embodiment of the present invention.

Figures 1F and 1G illustrate linear and branched access level requirements that are accounted for by the invention.

Figure 2 is a flow chart of a signature authorization method according to the present invention.

Figure 3 is a flow chart of a content filtering method according to the prior art.

5 Figure 4 is a block diagram of a content element according to the prior art.

Figure 5 is a flow chart of a content receiver method according to the prior art.

DETAILED DESCRIPTION OF A PREFERRED MODE

10 Figure 1A is a flow chart of an e-mail and content filtering method 99 according to the present invention. In particular, according to the present invention, a first user (i.e., "user one") prepares 100 selected content (e.g., without limitation, an e-mail message) for transmission to users or recipients within or without a selected entity or organization. According to one
15 embodiment of the present invention, a pool or group of potential recipients or candidate recipients is pre-established and identified by membership (or employment) within a particular organization or entity. The members have received the public and private encryption keys of the entity as well as the public key of a trusted certification authority within the entity. The content to be
20 transmitted is processed with a predetermined encryption algorithm and the entity private key to generate an identifying signature which according to one embodiment of the present invention is embedded or otherwise integrated or associated with the content being transmitted. According to one embodiment of the present invention, the signature is secured in the header line of an e-mail
25 message to be transmitted. According to another embodiment of the present invention, the one or more selected signatures are embedded or distributed within one or more regions of the selected content to be transmitted. According to yet another embodiment of the present invention, a digital signature is integrated with selected portions of the content to be transmitted according to a
30 predetermined algorithm. After a particular item of selected content has been provided or integrated with a particular signature or signatures, the content item is transmitted, broadcast, or distributed 101 to addressable and non-addressable nodes, switches, bridges, routers and networks (local, wide, metropolitan, or

Internet, without limitation). After transmission, a second user (i.e., "user two") detects, reads, or receives 102 all or a portion of the transmitted content and the associated signature, and initiates content filtering operations according to the present invention. Such filtering operation according to one embodiment of the present invention includes determining 103 whether the received content portion includes a signature at all and then whether the signature is a valid one.

According to the present invention, the signature is valid if it can be decrypted to produce information which is coincident with a predetermined authentication reference. If a signature is present and valid, then the content portion or the entire message is stored 104 in a primary buffer or memory location or region which has priority and is thus readably available to the receiving user. The priority criterion may include such factors as convenience, accessibility, order in a listing, or proximity for data accessing, by way of an example without limitation. If a signature is found not to be valid as to the present entity after an assessment has been conducted, then the affected content portion associated with the invalid signature is stored or retained 105 in a secondary buffer or memory location or region having lower priority and which is not immediately available or accessible to the receiving user. For example, the members of the secondary buffer may be arranged numerically to follow in order after the members of a primary buffer of a listing of a preestablished e-mail mailbox.

Figure 1B is a block diagram of a computer network including a processing system which can be used with content filtering according to the present invention. In particular, computer network 129, according to one embodiment of the present invention, includes a network 130 (e.g., the Internet) and a first user node 131 (e.g., user one) at which the first user develops or stores selected content 132 for distribution with one or more embedded or integrated signatures according to the present invention. Computer network 129 further includes an "nth" user node 133 to which content may be transmitted and from which content may be received. Computer network 129 further includes a computer processing system 134 in turn having a content association filter and certification apparatus (CAFCA) 140 according to the present invention, a user interface 145 connected to the CAFCA 140, a buffer 146 for holding or retaining filtered content, and a buffer 147 for holding or retaining residue content which

either did not contain any signature or did not contain a valid signature. Computer network 129 further includes a second user node (e.g., user two) 135. User two 135, according to one embodiment of the present invention, is connected to CAFCA 140 through user interface 145 in order to access or read content in buffer one 146 and/or buffer two 147. According to one embodiment of the present invention, user two 135 has direct memory addressing (DMA) access to buffers 146 and 147. According to one embodiment of the present invention, buffers 146 and 147 are combined in a single memory and the contents of buffer 147 are arranged to follow the contents of buffer 146 in order of accessibility.

Figure 1C is a block diagram of a content item 150 according to the present invention. In particular, content item 150 includes a digital signature 151, selected content 152, a filtering agent 153 for auto registration of signature authorized users, and a register 154 of users having signature access to particular content. According to the present invention, when a content item 150 is received by a second user or a processor associated with a second user, filtering agent 153 which contains a computer program product to enable installation and self configuration of a content association filter apparatus effective for identifying second users entitled to signature access to particular content is activated.

The register 154C in Figure 1C receives an information item (document, memorandum data, etc.) and examines an access level indicator 155 associated with the item. The access level indicator 155 identifies or refers to the associated information item and sets forth an access level signature that must be presented in order for a user to obtain access to that item. The spectrum of access levels may be a linear arrangement in which, for any two distinct access levels,, one of the two access levels (level 1) is always "greater than" the other access level (level 2); the levels 1 and 2 are said to be comparable and are illustrated in Figure 1F. Alternatively, the spectrum of access levels may have parallel branches in which two distinct access levels can be found for which neither level can be said to be "greater than" the other level; the two access levels are not comparable, because neither level can be compared to the other level in a linear format of access levels, as illustrated in Figure 1G.

When an e-mail system grants access to a specified e-mail message (e.g., for display, presentation to a user, incorporation into a folder, electronic downloading, provision of a hard copy, automatic display or execution of an attached document, etc.), the e-mail system also checks the e-mail message access level indicator. The system either authenticates the asserted access level or rejects the asserted access level. If the access level is authenticated, the system identifies the access level and checks this level against an access level that is required for processing the message (for display, etc.).

At least three situations are possible: the system confirms that the access level presented is at least as high as the required access level; (2) the system confirms that the access level presented is not as high as the required access level and denies access and/or logs the event; and (3) the system determines that the presented access level and the required access level are not comparable (e.g., the situation is as illustrated in Figure 1G), notifies the user and/or a competent authority of this situation and does not, at that time, permit the access. If a competent authority subsequently examines the situation and determines that access should be granted by the system, the competent authority transmits an authorization, which is preferably authenticated by the system, to grant or perform the access.

Access levels may include any or all of the following restrictions on access instrumentality, or method of receiving the message: (1) display only; (2) electronic downloading; (3) provision of a hard copy; (4) automatic display of attached document(s); and (5) automatic execution of attached file(s). Optionally, one or more of these access instrumentality levels requires presentation and authentication of an asserted access instrumentality level that must be at least as high as the access instrumentality level proposed to be used to present the message to the intended recipient.

It is possible to configure or define the access levels across an organization, based on the behavior of the particular e-mail system that performs or denies access, and/or based on requirements for individual users. An individual user can vary his/her access level requirements, increasing or decreasing the required access level depending upon the circumstances. For example, an individual could deny level 5 access for his/her own e-mail, in order

to minimize the likelihood of successful execution of a computer virus associated with an e-mail message. This configuration provides flexibility in establishing, securing and controlling an organization's e-mail.

The sequence (or a selected subsequence) of restrictions on instrumentality for access may be imposed by the system based on a comparison of the user access level, the required information item access level and other relevant information, and is preferably imposed after the system determines that the user is entitled to have access to the requested information item.

Figure 1D is a block diagram of a computer system 160 which can be used as a computer processing system for filtering content and certifying signatures in accordance with the present invention. Computer system 160 particularly includes a random access memory (RAM) 170; a read only memory (ROM) 171; a memory bus 172 connected to RAM 170 and ROM 171; a microprocessor 173 connected to the memory bus 172; a monitor 176; a printer 177; a disk drive 178; a compact disk read only memory (CD ROM) drive 179; a peripheral bus 180 connected to monitor 176, printer 177, disk drive 178, and CD ROM drive 179; a hard drive 181; and a network interface, each connected to peripheral bus 180 as shown in Figure 1D. Disk drive 178 and CD ROM drive 179 are respectively able to read information including computer program products (not shown) which can be embedded on media such as, respectively, a magnetic or optical disk or floppy 178' and a CD ROM medium 179'. Depending upon the selected drive and medium, writing on the selected medium as well as reading can be accomplished.

Figure 1E is a block diagram of a content association filter and certification apparatus (CAFCA) 140 according to one embodiment of the present invention. In particular, CAFCA 140 according to one embodiment includes a filter device (FD) 189 for filtering incoming content to determine its status as authorized or unauthorized for example, a certification device (CD) 190 for certifying outgoing content by applying a signature based upon a private key and an encryption algorithm as discussed below, a cryptographic coding engine (CCE) 191 connected to FD 189 and CD 190, and a local storage memory (LSM). The CCE 191 contains and provides a predetermined algorithm (such as DSA) for signature decryption by FD 189 and for signature creation by CD 190,

invention, a CAFDA 140 can have either an incoming content filter device 190 or an outgoing content certification device 191 or both. Incoming content filter device 190 filters content received from another user within the same or another network, according to the present invention by checking for the presence or absence of a header or signature. If a header is present identifying an acceptable source, the authenticated content is retained or stored preferentially.

Alternatively, if a signature is detected identifying (after decryption) an acceptable source, then again the content is considered acceptable for segregation or other preferential treatment. Outgoing content certification device 191

provides a signature, according to the present invention, to outgoing content to enable recipient users in the same or another network to conduct a filter operation, according to the present invention, to determine whether the content received is legitimate, high priority content and not non-authorized spam which can be discarded or set in a lower priority buffer or memory region. More

particularly, content certification device 191 according to one embodiment of the present invention is configured to receive and store a private key of an individual or entity. According to one embodiment of the present invention, a digital signature is a group of bits which can be analyzed to produce a validating result authenticating a purported source individual or entity providing the signature as an identifying mark. The digital signature is self-authenticating and it further

validates any content associated with the signature as content of the individual or entity performing the signing act. A digital signature is created according to one embodiment of the present invention by encrypting selected content wholly or partially with which the signature is to be linked, by using an entity or individual private key according to a selected encryption algorithm. According to one

embodiment of the present invention, a signature is generated by CD 191 according to the Digital Signature Algorithm (DSA) proposed by the U.S. National Institute of Standards and Technology on 30 August 1991 in the Federal Register, pp. 42980-42082. A DSA signature according to one embodiment includes a pair of large numbers represented in a computer by strings of binary digits. The digital signature according to this embodiment is compiled with a series of computational rules according to the DSA algorithm and a set of parameters to make it possible to certify both the identity of the signatory person

or entity and the integrity of the data as verifiably free of tampering. The DSA algorithm thus makes it possible to generate and verify signatures. In particular according to the DSA algorithm, a digital signature is generated by using the DSA and a selected private key of an individual or entity to encrypt selected content. An e-mail message is the combination of the signature and the unencrypted content, where the signature itself is an embodiment of an encrypted form of the content. Accordingly, tampering of the content can be detected by comparing the decrypted content within the signature (which is a regeneration of the original content) with the received unencrypted content transmitted in connection with the signature. Encryption is accomplished according to the present invention by applying the DSA algorithm (for example) with a particular private entity or individual key, such as PREK 193 example. Decryption of the signature is accomplished by applying the public key (i.e., PUEK 194) available to the entity recipient of the message or e-mail according to one embodiment of the present invention. The parameters of the DSA algorithm used according to the present invention include (1) a prime number p such that $2^{L-1} < p < 2^L$ for $512 \leq L \leq 1024$ and $L = 64 * (\text{alpha})$ for any alpha; (2) a prime number q such that $2^{159} < q < 2^{160}$ and $p-1$ is a multiple of q ; (3) a number g of order $q * (\text{modulo}(p))$ such that $g = h^{[(p-1)/q]} * (\text{modulo}(p))$, where h is any integer such that $1 < h < p-1$ and $g = h^{[(p-1)/q]} * (\text{modulo}(p)) > 1$; (4) a private key which is a number x generated pseudorandomly or randomly; (5) a public key which is a number y such that $y = g^x * (\text{modulo}(p))$; and (6) a number k generated pseudorandomly or randomly such that $0 < k < q$. The integers p , q , and g are parameters which are shared by communicating users employing the DSA algorithm, according to one embodiment of the present invention. The private and public keys are x and y respectively used for coding and decoding. The parameters x and k are used to generate signatures for use in accordance with the present invention, and the parameter k is regenerated for each signature. A user who wishes to engage in encryption for constructing a digital signature which will be transmitted with selected content creates a signature according to one embodiment of the present invention by computing $r = (g^k * (\text{modulo}(p))) * (\text{modulo}(q))$ and $s = [(m + xr)/k] * (\text{modulo}(q))$ where k is $\text{modulo}(q)$. The signature is thereupon verified by computing $w = [1/s] * (\text{modulo}(q))$; $u_1 = mw * (\text{modulo}(q))$; $u_2 = rw * (\text{modulo}(q))$;

$v = (g^{u1} y^{u2} \text{ modulo}(p)) * \text{modulo}(q)$; and comparing v and r for equality to determine whether the signature is or is not authentic. Accordingly, the PREK 193 is used to create a signature of the individual or entity with the DSA algorithm according to one embodiment of the present invention. The signature is created for example by encrypting the entire content or information to be transmitted with the DSA algorithm using the PREK 193. Alternatively, selected or randomly determined portions of the content are encrypted with the DSA or another cryptographically strong algorithm to generate the signature. The signature is then transmitted with the unencrypted version of the content. When the signature is decrypted, another version of all or part of the content is available for tamper comparison with the received unencrypted content. In particular, selected bits or all of the decrypted content is compared with the unencrypted content. If there are differences, tampering or other errors are presumed to have occurred, causing the information recipient to be on guard and to undertake separate content authentication or assurance procedures.

Content certification device 190 may additionally receive and store the public key of a certification authority from which entity public and private keys may be received on a one time basis or on multiple occasions. With this public key, messages and new entity and private keys can be securely received from the certification authority of a particular entity. Filter device 190 according to one embodiment of the present invention filters received information and content by receiving and classifying information received, by determining whether the information includes an indication of local origin, and by assigning priority to any local origin received information. The information received according to one embodiment of the present invention includes selected subject matter and header content. The header content according to one embodiment of the present invention is a header line. According to one embodiment of the present invention, the filter device 190 discriminates and classifies information based upon origin information identified in the header or in any other portion of the information received. Alternatively, local origin is determined by decrypting a sender signature to produce secure content for comparison with the content subject matter provided with the signature. Alternatively, local origin is

determined by the presence of the senders authenticable private key which has been encrypted into the signature.

Figure 2 is a flow chart of a signature authorization method 259 according to the present invention. According to one embodiment of the present invention, method 259 includes determining whether to select 260 individual or entity certification of a particular item of content to be transmitted. Individual certification provides the selected item of content with an individual imprimatur or signature identifying the selected content as being identified with a particular individual. Entity or group certification provides the content with a signature associating the selected content with the particular group or entity. If individual certification is to be accomplished, then the particular content item is provided 261 with the signature of the certifying individual. The signing action can, according to one embodiment of the present invention, entail executing, embedding, or integrating a signature on or in the content with the private key of the individual or entity, for example. Next, a determination is made 262, according to the present invention, whether the entity certification is to be accomplished with an individual key or with a group or entity certification. If an individual signature is needed, then the entity with which the individual is associated certifies 264 the individual signature according to one embodiment of the present invention. If no individual signature or key is desired, the entity itself or a representative of the entity accomplishes 263 signature on behalf of the particular entity. According to one embodiment of the present invention, the entity certifies private and public keys of the entity by providing each private key of the entity to the members of the entity in encrypted form, using a second entity private key having a public counterpart already known to the members to enable decryption of the new entity public and private keys.

Figure 3 is a flow chart of a content filtering method (CFM) 299 according to the prior art. In particular, a Usenet news group (UNG) 300 posts news to a selected list of news groups. UNG 300 uses Pretty Good Privacy (PGP) Moose monitoring 301 of particular postings and authenticating the postings even if the postings are modified by preprocessing. A determination is next made 302 under CFM 299 whether to enable automatic or discretionary cancellation of posted messages. Under a discretionary embodiment according to

the prior art, each posting is individually approved by UNG 300. However, in an automatic mode of the prior art, forged or unapproved content (i.e., unsigned) content and messages are cancelled automatically.

Figure 4 is a block diagram of a content element 399 according to the prior art. In particular, an item of content 399 includes, according to the prior art, content material 400, a header 401 in turn including a signature 402. The signature 402 in turn includes a name 410, an identification (ID) code 411, and a password 412, according to one approach.

Figure 5 is a flow chart of a content receiver method according to the prior art. In particular, according to one embodiment of the present invention, when a content element or item is received after transmission it is checked 501 for a header. Next, a determination is made whether the content received has been subject to tampering 502. If yes, further processing of the content stops 503 as the veracity of the content will have been called into question. In the absence of any identified content tampering, signature authentication is performed 504, to determine the validity of the signature as identifying the source or distributor or the particular content.

WHAT IS CLAIMED IS:

1. A method for filtering information received from an asserted source, the method comprising:

- 5 receiving selected information including an asserted source of the information and an encryption-created authentication signature of the asserted source;
- determining whether the signature is authentic; and
- when the signature is determined to be authentic, applying the selected
- 10 information to a preferred information buffer.

2. The method of claim 1, further comprising:

- when said signature is determined to be not authentic, applying said selected information to a non-preferred information buffer.

3. The method of claim 1, further comprising:

- when said signature is determined
- to be not authentic, declining to process selected information further.

4. The method of claim 1, further comprising providing an authentication signature for content of said selected information.

5. Apparatus for filtering information received from an asserted source, the apparatus comprising a computer that is programmed:

- 25 to receive selected information including an asserted source of the information and an encryption-created authentication signature of the asserted source;
- to determine whether the signature is authentic; and
- when the signature is determined to be authentic, to apply the selected
- 30 information to a preferred information buffer.

6. The apparatus of claim 5, wherein said computer is further programmed so that, when said signature is determined to be not authentic, said selected information is applied to a non-preferred buffer.

5 7. The system of claim 5, wherein said computer is further programmed so that:

 when said signature is determined to be not authentic, to decline to process selected information further.

10 8. The apparatus of claim 5, wherein said selected information includes an authentication signature for content of said selected information, and said computer is further programmed to determine whether the signature for the information content is authentic.

15 9. A method for filtering information received by e-mail, the method comprising:

 receiving an e-mail message for a specified recipient, including a signature for an asserted source and an asserted access level for the message;

20 determining whether the signature for the asserted source and for the asserted access level is authentic;

 when the signature is determined to be authentic, comparing the asserted access level with a required access level for the recipient; and

 taking at least one of the following actions:

25 when the asserted access level is at least as great as the required access level, permitting the message to be accessed by the recipient;

 when the asserted access level is less than the required access level, withholding access by the recipient to the message; and

 when the asserted access level and the required access level are not comparable, referring the question of access by the recipient to the message to a selected authority for e-mail access.

30

10. The method of claim 9, further comprising:

when said signature is determined to be not authentic, declining to permit access by said recipient to said message.

5 11. The method of claim 9, further comprising:

providing said e-mail message with an asserted instrumentality access level and with a signature for the asserted instrumentality access level;

determining whether the instrumentality access level signature for the asserted source is authentic;

10 when the instrumentality access level signature is determined to be authentic, comparing the asserted instrumentality access level with a required instrumentality access level for the recipient for at least one access instrumentality; and

15 when the asserted instrumentality access level is at least as great as the required instrumentality access level for the at least one access instrumentality, permitting said message to be accessed by said recipient using the at least one access instrumentality.

12. The method of claim 11, further comprising:

20 when said asserted instrumentality access level is not at least as great as said required instrumentality access level for said at least one access instrumentality, declining to permit said message to be accessed by said recipient using said at least one access instrumentality.

25 13. The method of claim 11, further comprising choosing said at least one access instrumentality from a group of access instrumentalities consisting of: message display only; electronic downloading of said message; provision of a hard copy of said message; automatic display of at least one document associated with said message; and automatic execution of at least one file associated with
30 said message.

14. A system for filtering information received by e-mail, the system comprising a computer that is programmed:

to receive an e-mail message for a specified recipient, including a signature for an asserted source and an asserted access level for the message;

to determine whether the signature for the asserted source and for the asserted access level is authentic;

5 when the signature is determined to be authentic, to compare the asserted access level with a required access level for the recipient; and

to take at least one of the following actions:

when the asserted access level is at least as great as the required access level, to permit the message to be accessed by the recipient;

10 when the asserted access level is less than the required access level, to withhold access by the recipient to the message; and

when the asserted access level and the required access level are not comparable, to refer the question of access by the recipient to the message to a selected authority for e-mail access.

15

15. The system of claim 14, wherein said computer is further programmed so that:

when said signature is determined to be not authentic, to decline to permit access by said recipient to said message.

20

16. The system of claim 14, wherein said computer:

to provide said e-mail message with an asserted instrumentality access level and with a signature for the asserted instrumentality access level;

25 to determine whether the instrumentality access level signature for the asserted source is authentic;

when the instrumentality access level signature is determined to be authentic, to compare the asserted instrumentality access level with a required instrumentality access level for the recipient for at least one access instrumentality; and

30 when the asserted instrumentality access level is at least as great as the required instrumentality access level for the at least one access instrumentality, to permit said message to be accessed by said recipient using the at least one access instrumentality.

17. The system of claim 16, wherein said computer is further programmed so that:

when said asserted instrumentality access level is not at least as great as said required instrumentality access level for said at least one access instrumentality, to decline to permit said message to be accessed by said recipient using said at least one access instrumentality.

18. The system of claim 16, wherein said computer is further programmed to choose said at least one access instrumentality from a group of access instrumentalities consisting of: message display only; electronic downloading of said message; provision of a hard copy of said message; automatic display of at least one document associated with said message; and automatic execution of at least one file associated with said message.

ABSTRACT OF THE DISCLOSURE

A digital signature is embedded in the header of selected content to be transmitted. A recipient of the content identifies the priority of the content according to header line content or signature presence and segregates signed
5 priority content from non-authenticated content. Signature generation and filtering as well as certification are accomplished by running application specific software on a selected computer. Required e-mail access level may vary with the intended recipient and/or with the instrumentality by which e-mail access is
10 allowed.

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
220

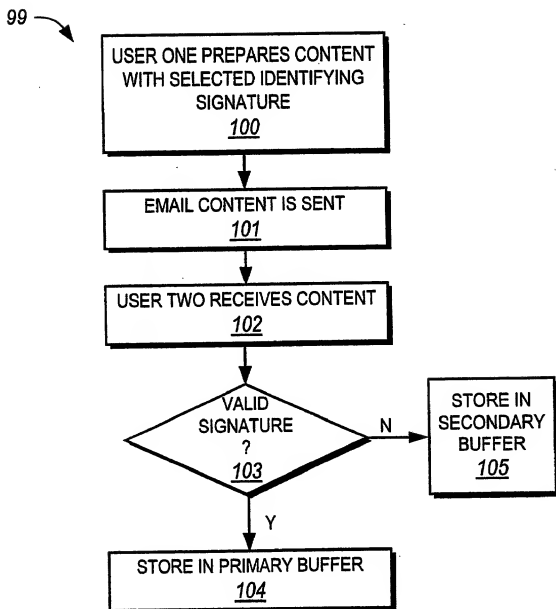


FIG. 1A

129 →

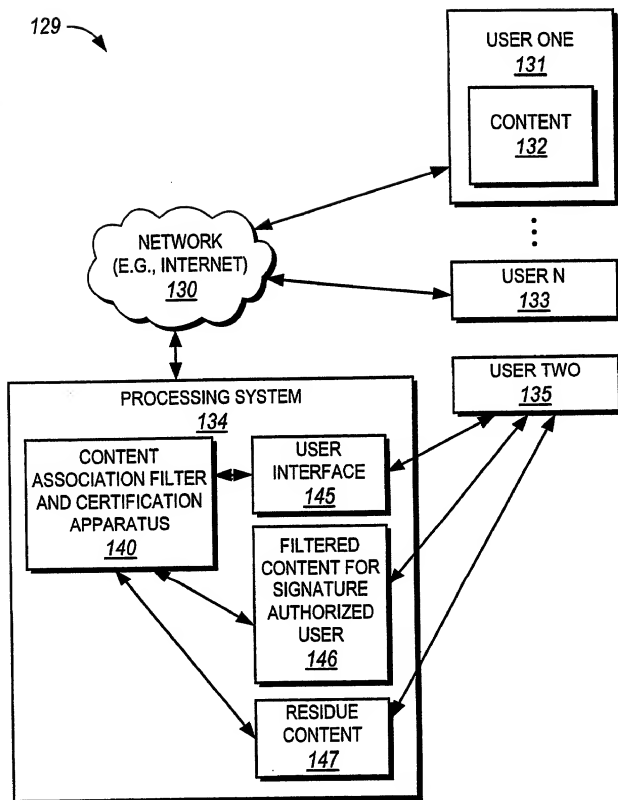


FIG. 1B

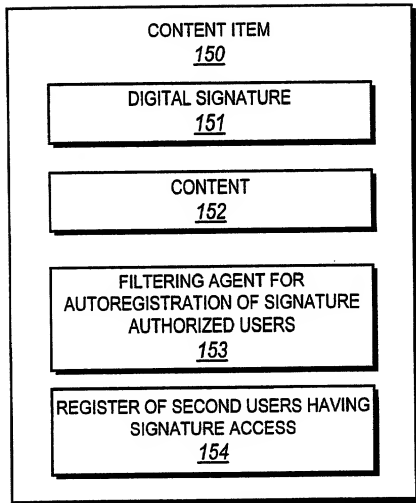


FIG. 1C

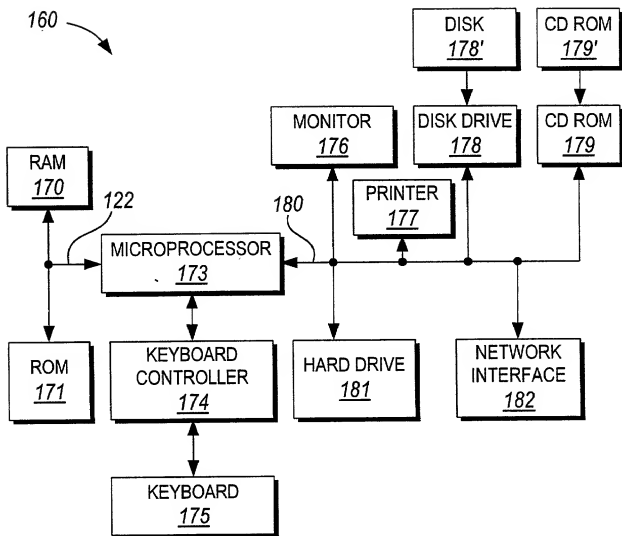


FIG. 1D

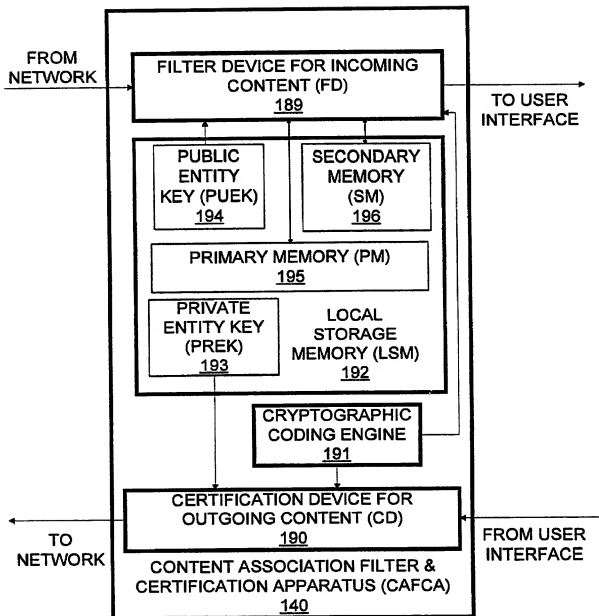


FIG. 1E

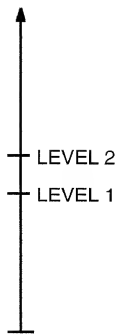


FIG. 1F

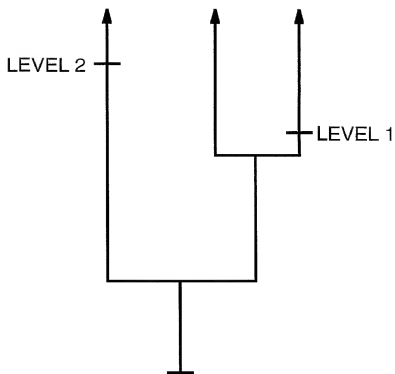


FIG. 1G

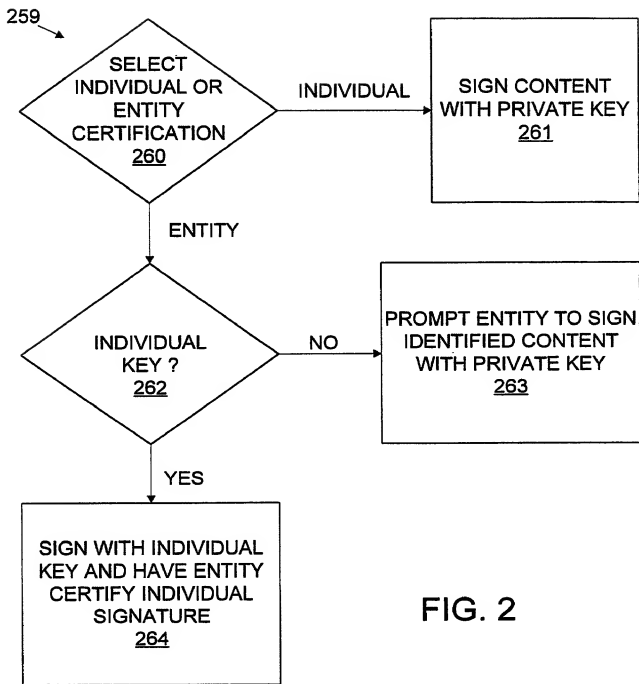


FIG. 2

299

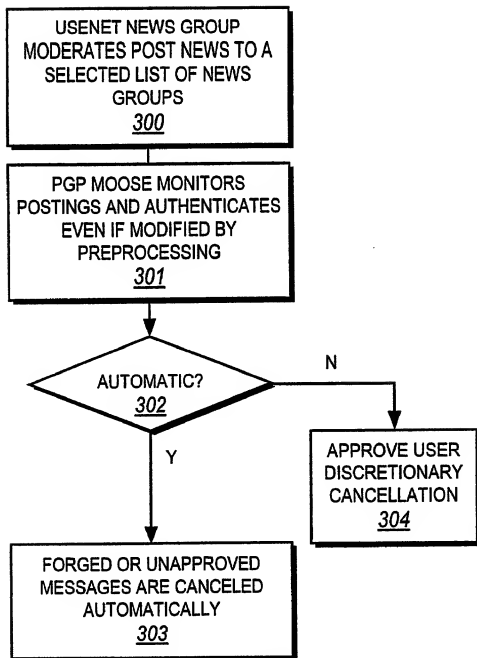


FIG. 3
PRIOR ART

399

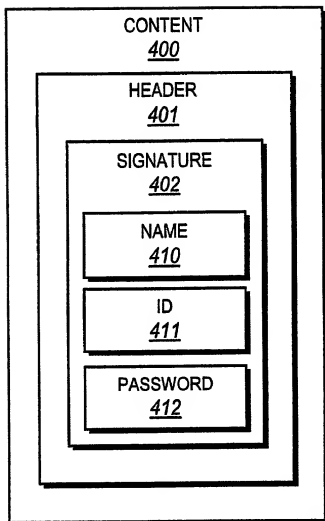


FIG. 4
PRIOR ART

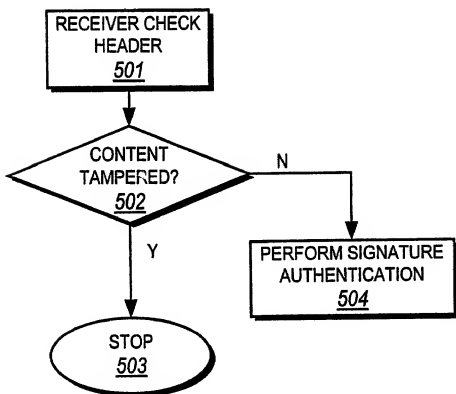


FIG. 5
PRIOR ART

99

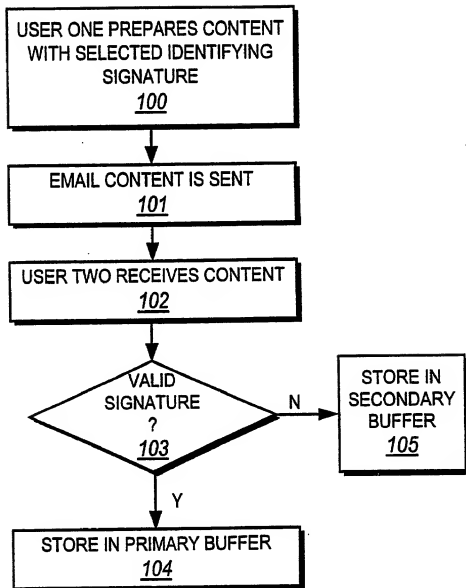


FIG. 1A

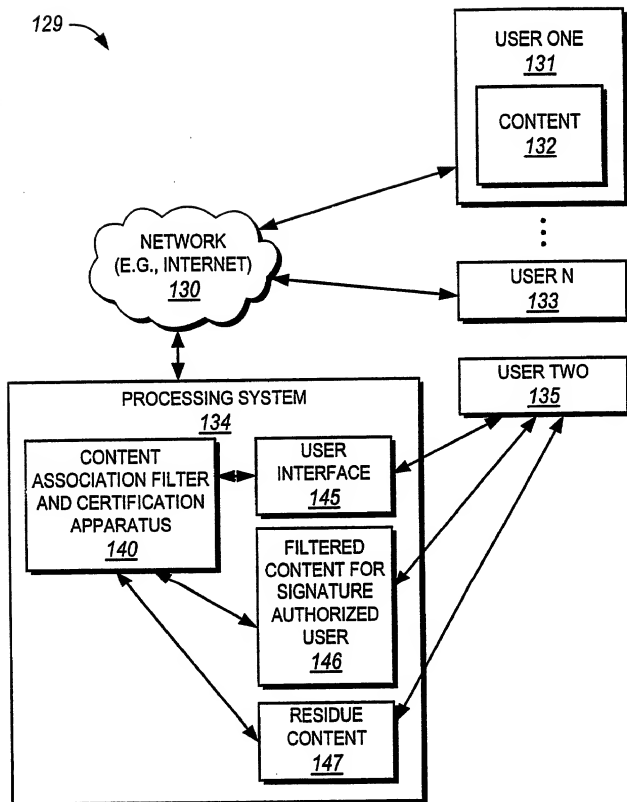


FIG. 1B

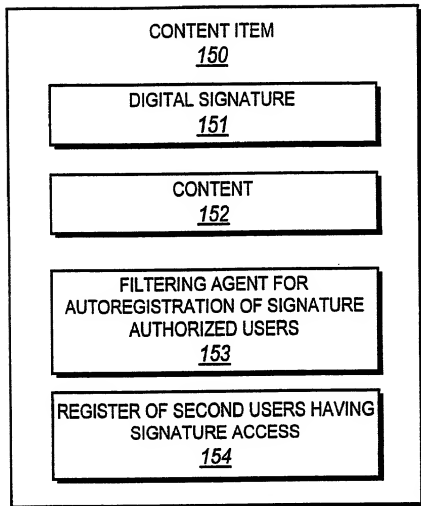


FIG. 1C

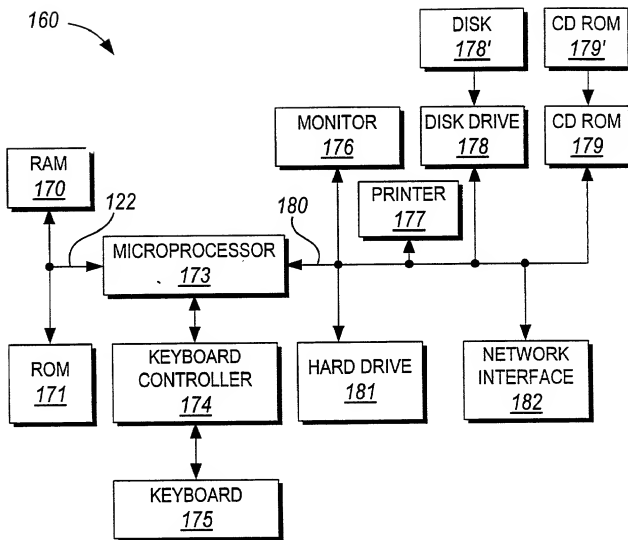


FIG. 1D

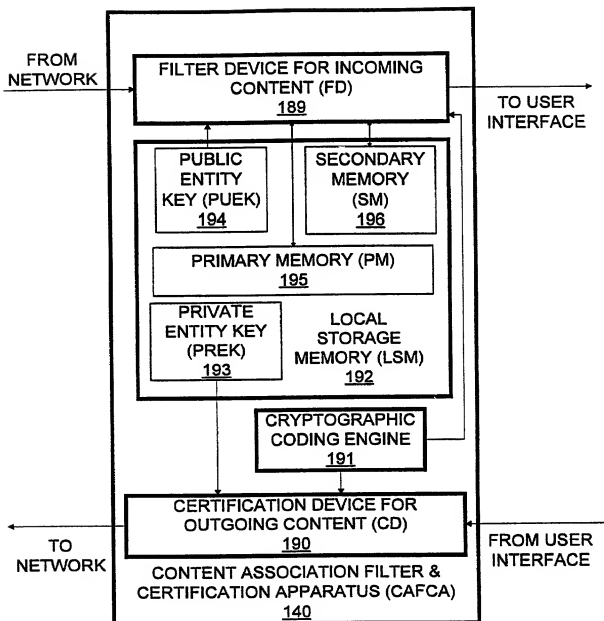


FIG. 1E

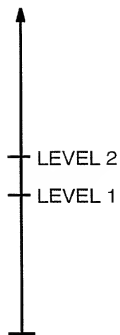


FIG. 1F

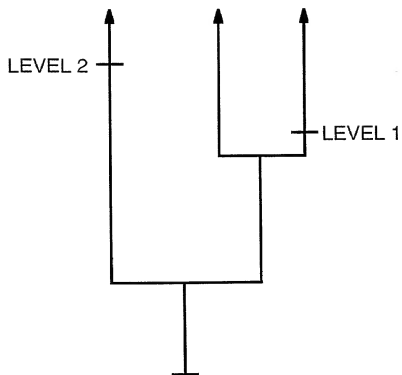


FIG. 1G

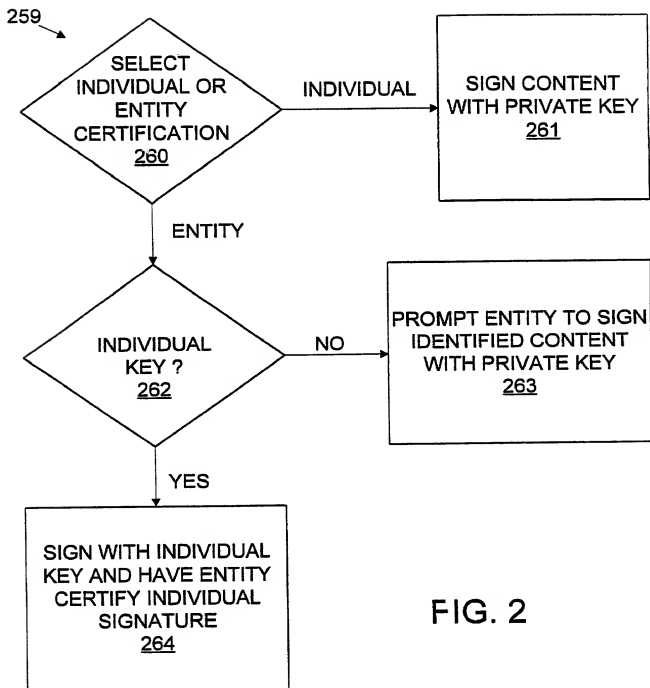


FIG. 2

299 →

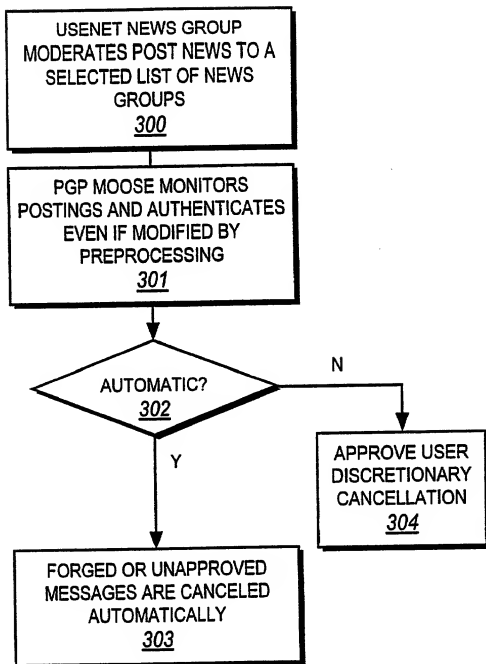


FIG. 3
PRIOR ART

399 →

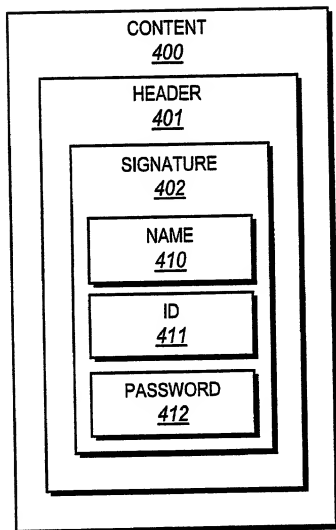


FIG. 4
PRIOR ART

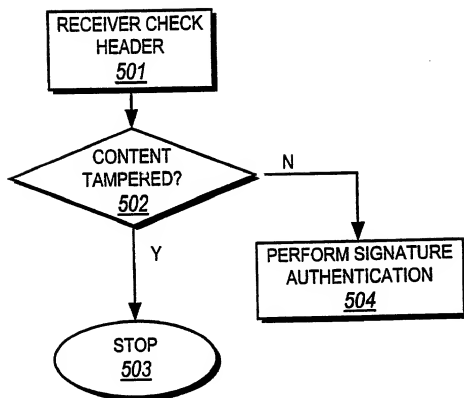


FIG. 5
PRIOR ART

PATENT APPLICATION

DECLARATION AND POWER OF ATTORNEY
Original Application

As below named inventor, I declare that I have reviewed and understand the contents of the specification, including the claims, as amended by any amendment specifically referred to in this Declaration, that the information given herein is true, that I believe that I am the original and first inventor of the invention entitled:

APPARATUS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR FILTERING INFORMATION

which is described and claimed in:

X the attached specification or

— the specification in application Serial No. _____ filed _____.

X The present application is a continuation-in-part of Prior Application Serial No. 08/946,036 filed October 7, 1997, and may be considered to disclose and claim subject matter in addition to that disclosed in the Prior Application, and I hereby claim the benefit of 35 U.S.C. Section 120.

that I acknowledge my duty to disclose information in accordance with 37 C.F.R. Section 1.56 and defined on the attached sheet, which is material to the examination of this application, that I do not know and do not believe the same was ever known or used in the United States of America before my or our invention thereof or patented or described in any printed publication in any country before my or our invention thereof, or more than one year prior to this application, or in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application and that as to applications for patent or inventor's certificate filed by me or my legal representatives or assigns in any country foreign to the United States of America, the earliest filed foreign application(s) filed within twelve months prior to the filing date of this application and all foreign applications filed more than twelve months prior to the filing date of this application, if any, are identified below.

CHECK APPROPRIATE BOX

X No earlier-filed foreign applications.

— Required information as to foreign applications filed prior to filing date of this application is on page 5 attached hereto and made a part hereof.

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

<u>NAME</u>	<u>REGISTRATION NO.</u>	<u>NAME</u>	<u>REGISTRATION NO.</u>
Kenneth Olsen	26,493	John F. Schipper	26,994
Timothy J. Crean	37,116	Stanley N. Protigal	28,657
Robert S. Hauser	37,847	Richard E. Bee	18,005
Joseph T. FitzGerald	33,881	of Law Office of John Schipper	
Alexander E. Silverman	37,940		
Christine S. Lam	37,489		
Anirma Rakshpal Gupta,	38,275		
Sean Patrick Lewis	42,798		
Michael J. Schallop	44,319		
Bernice B. Chen	42,403		
Kenta Suzue	45,145		
Noreen A. Krall	39,734		
Richard J. Lutton, Jr.	39,756		
Monica D. Lee	40,696		
Marc D. Foodman	34,110		
of SUN MICROSYSTEMS, INC.			

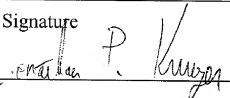
SEND CORRESPONDENCE TO
Law Office of John Schipper
111 N. Market Street, Suite 808
San Jose, California 95113

DIRECT TELEPHONE CALLS TO

Tel: 408/293-9934
Fax: 408/293-2183

(201) FULL NAME OF INVENTOR	LAST NAME KRUEGER	FIRST NAME JONATHAN	MIDDLE NAME P.
RESIDENCE & CITIZENSHIP	CITY PLEASANTON	STATE OR FOREIGN COUNTRY CALIFORNIA	COUNTRY OF CITIZENSHIP U.S.
POST OFFICE ADDRESS	POST OFFICE ADDRESS 4631 GATETREE CR.	CITY PLEASANTON	STATE OR COUNTRY U.S
			ZIP CODE 94566

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Name (201) JONATHAN P. KRUEGER	Signature 	Date 10 August 2000
------------------------------------------	--------------------------------------------------------------------------------------------------	-------------------------------

IN WITNESS WHEREOF, I have hereunto set my hand and seal on the date indicated below:

Date: 10 Aug 2006

Jonathan P. Krueger
Jonathan P. Krueger

LAW OFFICE OF JOHN SCHIPPER
111 North Market Street, Suite 808
San Jose, California 95113